경력 기술서

박재하

회사명	국방과학연구소(ADD) / 2본부 3부 5팀·2팀·4팀	
근무기간	2016.07.18 ~ 2019.07.24 (3년)	
주요업무	해킹/방어 기술 연구, 모의 해킹, 취약점 분석, 보안SW 개발, 악성코드 개발	
업무내용	5팀	- 취약점 자동 분석기술 연구 (Fuzzing, Taint Analysis 등) - 논문: "기본 블록 확장을 통한 !exploitable 개선", 한국정보과학회, 1066~1068, 2017. - 美 사이버작전 교리(JP 3-12) 분석 및 기술번역 - 사이버 전문인력 대상 시스템 해킹 교관 (가상환경 구성 및 교안 저술, 실습교육)
	2팀	- 敵 대상 정보수집 기술 연구 및 외주개발업체 관리 (Python / selenium, bs4) - 敵 OS, 워드프로세서를 대상으로 한 문서형 악성코드 개발 (Assembly / BOF, ROP, RTL) - 관련 사업관리(SRR, SDR, CDR, TRR 등) 및 산출물 저술, 소요군 대상 시험평가 수검
	4팀	- 침입감내시스템 소스코드 리뷰 및 토의 (C++ / Xen Hypervisor 등) - ML기반 침입탐지기술 연구 세미나 (관련 기술 리서치 및 발표) - ML 네트워크침입탐지시스템 알고리즘 개발 (Python / nDPI, ELK stack, tensorflow) - 논문: "비지도학습을 이용한 네트워크 정상상태 모델링 기법", 한국군사과학기술학회, 1330~1331, 2019 - 논문: "네트워크 프로토콜 분류 및 특징정보 추출 기법 연구", 한국군사과학기술학회, 1431~1432, 2019
	출장/ 파견	- ADD MDM(Mobile Device Management) 앱/서버 취약점 분석 (Java, PHP) - 국방망 웹응용체계 대상 모의해킹 (훈련 파견) (JS, PHP, MySQL 등)

회사명	공군 사이버작전센터 / 정보보호대
근무기간	2019.07.29 ~ 2020.01.10 (6개월)
주요업무	침해대응(대응반장), 공개취약점 조치·관리, 정보보호장비 정책 설정·관리
업무내용	- 공군 전체 대상 예하 CERT 통제, 공개취약점 조치 및 관리, FW·IPS·NAC 정책 관리 등 - NAC 스크립트 실행기능 활용 PMS 기능 개발 (VBS, MS-DOS / 윈도우 및 크롬 업데이트) - 훈련 대응을 위한 IPS 룰 제작 및 적용 (Snort Rule / 공격자 패턴기반 차단)

회사명	국군방첩사령부 (舊 군사안보지원사령부 또는 국군기무사령부) / 국방보안연구소
근무기간	2020.01.13 ~ 2020.12.31 (1년)
주요업무	한국형사이버보안위험관리제도(K-RMF) 개발
업무내용	- 美 위험관리제도 분석(SP 800-37, 53, 53A 등) 및 번역, 관련 표준 분석(CCI, STIG/SRG 등) - 한국군 관련 법·훈령 비교분석 및 관련 해킹/방어기술 및 보안시스템공학 문서 리서치 - 한국형사이버보안위험관리제도(K-RMF) 보안통제항목(Security Controls) 및 준수 가이드 저술

회사명	국군지휘통신사령부 / 80대대 운용과, 사령부본부 C4I방호처 전장체계과·사이버방호과
근무기간	2021.01.04 ~ 2021.12.31 (1년)
주요업무	한국형사이버보안위험관리제도(K-RMF) 시범적용 추진
업무내용	- 시스템 담당자, 보안 관리자, 개발 및 유지보수업체 인터뷰 등 백데이터 수집 - 관련 내규 및 지침 검토, 문서이력 검토하여 근거자료 수집 및 관리 - 대상체계 RMF 산출물 작성 및 보완 (정보유형 분류, Security Plan, POA&M 등) - 타 부처/기관(국방부, 합참, 방첩사, 사이버사) 대응 및 K-RMF 시범평가 수검 - 취약점 후속조치 방안 작성 및 관리, 시스템 담당자 및 성능개량업체 등과 실무협의 - 국직부대 전체 대상 방화벽, NAC 정책 관리 및 CERT 업무지시

회사명	사이버작전사령부 (舊 국군사이버사령부) / RMF과, 무기체계안전대
근무기간	2022.01.03 ~ 2023.05.31 (1년 5개월)
주요업무	모의 해킹, 취약점 분석, K-RMF 시범적용 추진
업무내용	- 리눅스/유닉스 대상 보안설정점검 쉘 스크립트 리뷰 - 대상체계 K-RMF 시범적용 평가 수행 (정보분류 및 기준선 검토, 보안통제항목평가, 위험평가) - 대상체계 RMF 산출물 작성 및 검토 (SAP, SAR, RAP, RAR 등) - 국방부 K-RMF 임무분장 개선안 및 제도 발전방안 작성 및 대응, 관련 기술문서 리서치 - 대상체계 모의침투 및 취약점분석 수행 (네트워크장비·웹응용체계·단말기 대상 모의해킹) - 무기체계/정보체계 취약점 정기점검 (웹응용, 리눅스/유닉스 서버, DBMS, 단말기 등)